

WHAT IS CLAIMED IS:

- 1           1.       A client-server security system comprising:.  
2                a client system receiving first biometric data and having a first level security  
3        authorization procedure; and  
4                a server system receiving second biometric data and having a second level  
5        security authorization procedure;  
6                wherein the first level security authorization procedure and the second level  
7        security authorization procedure comprise distinct biometric algorithms.
- 1           2.       The client-server security system of claim 1 wherein the first biometric  
2        data comprises speech data.
- 1           3.       The client-server security system of claim 2 wherein the speech data  
2        comprises to a password.
- 1           4.       The client-server security system of claim 1 wherein the second  
2        biometric data comprises speech data.
- 1           5.       The client-server security system of claim 1 wherein the first level of  
2        security authorization comprises user verification.
- 1           6.       The client-server security system of claim 1 wherein the second level  
2        of security authorization comprises user identification.
- 1           7.       The client-server security system of claim 1 wherein the first level of  
2        security authorization comprises a neural network.
- 1           8.       The client-server security system of claim 1 wherein the second level  
2        of security authorization comprises Hidden Markov Models.
- 1           9.       A method of performing a secured transaction on a server system  
2        comprising:  
3                receiving a first level security authorization signal on the server system from a  
4        client system;  
5                receiving biometric data on the server system from the client system;

9 generating a second level security authorization signal on the server system  
10 when the first biometric algorithm indicates that the biometric data corresponds to one of a  
11 plurality of users authorized to access the server system.

12. The method of claim 9 further comprising re-executing the second level security authorization on the server system.

13. The method of claim 9 further comprising receiving control information from the client system.

14. The method of claim 13 wherein the control information comprises a verification confidence value.

1                   15. The method of claim 14 further comprising modifying an acceptance  
2 threshold of the first biometric algorithm in accordance with the verification confidence  
3 value.

1                   18.     The method of claim 13 wherein the control information comprises a  
2 authorization limitation criteria.

1                   19.     The method of claim 18 further comprising restricting access to remote  
2 resources in accordance with the authorization limitation criteria.

1                   20.     The method of claim 18 further comprising limiting allowable  
2 spending amounts in accordance with the authorization limitation criteria.

1                   21.     The method of claim 18 further comprising limiting allowable network  
2 connection time in accordance with the authorization limitation criteria.

1                   22.     The method of claim 9 further comprising providing access to a  
2 plurality of server resources in accordance with the first and second level authorization  
3 signals.

1                   23.     The method of claim 9 further comprising providing access to a  
2 plurality of remote network resources in accordance with the first and second level  
3 authorization signals.

1                   24.     The method of claim 9 further comprising executing an identification  
2 script to obtain identification information about the user.

1                   25.     The method of claim 9 further comprising retrieving biometric data  
2 from the client and storing the biometric data on the server for later identification of the user.

1                   26.     The method of claim 25 wherein the biometric data is a digital  
2 fingerprint.

1                   27.     The method of claim 25 wherein the biometric data is a digital voice  
2 print.

1                   28.     The method of claim 9 further comprising receiving a line quality  
2 measure in the server system, and in accordance therewith, selecting one of a plurality of  
3 server biometric algorithms for executing the second level security authorization.

1                   29.     The method of claim 9 further comprising receiving a line quality  
2 measure in the server system, and in accordance therewith, loading the first biometric

3 algorithm with a first input parameter value when the line quality measure is in a first range,  
4 and loading the first biometric algorithm with a second input parameter value when the line  
5 quality measure is in a second range.

1                   30. The method of claim 9 further comprising receiving a channel type  
2 signal in the server system, and in accordance therewith, loading the first biometric algorithm  
3 with a first input parameter value when the channel type has a first value, and loading the first  
4 biometric algorithm with a second input parameter value when the channel type has a second  
5 value.

1                   31. A method of performing a secured transaction on a client system  
2 comprising:

3                   receiving biometric data in the client system;

4                   analyzing a first portion of the biometric data using a first biometric algorithm  
5 on the client system;

6                   generating a first level security authorization signal on the client system when  
7 the first biometric algorithm indicates that the first portion of the biometric data corresponds  
8 to an authorized user;

9                   transmitting the first level security authorization signal and second portion of  
10 the biometric data to a server system, the second portion of biometric being analyzed by a  
11 second biometric algorithm on the server; and

12                   accessing resources on the server system through the client system when the  
13 second biometric algorithm provides a second level security authorization.

1                   32. The method of claim 31 further comprising generating a verification  
2 confidence value and transmitting the verification confidence level to the server system.

1                   33. The method of claim 32 further comprising modifying an acceptance  
2 threshold of the second biometric algorithm in accordance with the verification confidence  
3 value.

1                   34. The method of claim 32 further comprising transmitting second  
2 biometric data to the server system and analyzing the second biometric data using the second  
3 biometric algorithm when the verification confidence value is within a first range.

1                   35.     The method of claim 31 further comprising generating authorization  
2 limitation criteria and transmitting the authorization limitation criteria to the server system.

1                   36.     The method of claim 35 wherein the authorization limitation criteria  
2 comprises remote resource access restrictions.

1                   37.     The method of claim 35 wherein the authorization limitation criteria  
2 comprises spending amount limitations.

1                   38.     The method of claim 31 wherein the first portion of the biometric data  
2 is speech data and the first biometric algorithm is a speaker recognition algorithm.

1                   39.     The method of claim 38 wherein the speech data comprises a  
2 password.

1                   40.     The method of claim 31 wherein the second portion of the biometric  
2 data is speech data and the second biometric algorithm is a speaker recognition algorithm.

1                   41.     The method of claim 40 wherein the speech data comprises an  
2 utterance.

1                   42.     The method of claim 31 wherein client system is a portable media  
2 player.

1                   43.     The method of claim 31 wherein client system is a smart card.